CHAPTER 1

Product Overview

The Cisco MDS 9020 Fabric Switch offers Fibre Channel fabric-switching services that enable maximum performance and ensure high reliability. This switch combines robust and flexible hardware architecture and storage management intelligence. This powerful combination enables highly available, scalable storage networks that provide advanced security and unified management features.

The Cisco MDS 9020 Fabric Switch provides essential storage networking features that include advanced security, debug analysis tools, and unified SAN management.

This chapter lists the hardware features for the Cisco MDS 9020 Fabric Switch and describes its software features. It includes the following sections:

Hardware Overview

The Cisco MDS 9020 Fabric Switch provides these hardware features:

- 20 4-Gbps Fibre Channel ports per 1 RU
- Autodiscovery of Fibre Channel connections to single devices, loop devices, or other switches
- Autonegotiation of port transmission speeds of 1 Gbps, 2 Gbps, or 4 Gbps
- Port interfaces that support field-replaceable, hot-swappable, small form-factor pluggable (SFP) transceivers
- Front to back airflow
- Cisco MDS 9000 FabricWare software
- Full compatibility with the Cisco MDS 9000 Family

Refer to the *Cisco MDS 9020 Fabric Switch Hardware Installation Guide*.

Software Features

This section provides an overview of the major software features of the Cisco MDS 9020 Fabric Switch.

Switch Reliability

The Cisco MDS 9020 Fabric Switch maintains internally controlled reliability services that ensure continued service with no degradation. This reliability service includes the following functions:

- Provides power-on self testing (POST)
- Detects errors, isolates faults, performs parity checking, and checks illegal addresses
- Displays LEDs that summarize the status of the power supply and fan assembly

Intelligent Zoning

Intelligent zoning can control access between devices, and it accomplishes the following:

- Partitions devices that use different operating systems. In a heterogeneous environment, it is often necessary to separate servers and storage devices to avoid accidentally transferring information between devices with different operating systems. Such transfers could result in data corruption or deletion.
- Creates logical subsets of closed user groups. Closed user groups enforce security or to separate functional areas across the fabric.
- Configures groups of devices that are separate from the rest of the fabric. Based on the assigned zone membership, devices outside the zone cannot access devices inside the zone.
- Provides temporary access between devices (zone sets). Zone restrictions can be imposed temporarily and then restored to revert to normal operation, if desired.

See Chapter 7, “Configuring and Managing Zones.”

IP Services

The Cisco MDS 9020 Fabric Switch supports the following IP services:

- IP over Ethernet—These services are limited to traffic management.
- The Network Time Protocol (NTP) server—This server synchronizes the system clocks of network devices.

See Chapter 12, “Configuring IP Services.”

Switch Management Features

Along with the software features already listed, additional management features fall into these categories: fabric management and security management.

Fabric Management

The Cisco MDS 9020 Fabric Switch offers fabric management and control through the command-line interface (CLI) by using Telnet, SSH, or a serial console. The switch also offers fabric management through the Cisco MDS 9000 Family Fabric Manager tool by using Simple Network Management Protocol (SNMP):

- SNMP versions 1 and 2 are supported. See Chapter 9, "Configuring Switch Security."
- System log (syslog) messages are viewed through a console or Telnet session for asynchronous events such as an interface transition. System messages are directed to an internal log and optionally to an external server (refer to the *Cisco MDS 9020 Fabric Switch System Messages Reference)*. See Chapter 14, "Configuring System Message Logging."

Security Management

The Cisco MDS 9020 Fabric Switch offers secure switch management through user authentication and roles.

Switch Access Security

Each switch can be accessed through the CLI or SNMP.

- Secure switch access—Available when you explicitly enable Secure Shell Protocol (SSH) access to the switch. SSH access provides additional controlled security by encrypting data, user IDs, and passwords. By default, Telnet access is enabled on each switch.
- IP access control lists (IP-ACLs)—IP-ACLs enhance network security to the Cisco MDS 9020 Fabric. IP-ACLs restrict IP-related out-of-band management traffic based on IP addresses (Layer 3 and Layer 4 information). You can use IP-ACLs to control transmissions on management interfaces.

See Chapter 9, "Configuring Switch Security."

User Authentication

A strategy known as authentication, authorization, and accounting (AAA) verifies the identity of remote users, grant access, and tracks their actions. The Remote Access Dial-In User Service (RADIUS) provides a centralized AAA solution.

See Chapter 9, "Configuring Switch Security."

Role-Based Access

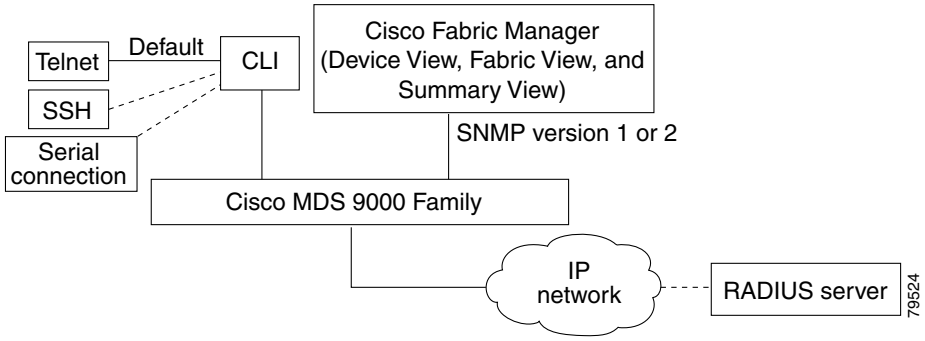
The Cisco MDS 9020 Fabric Switch performs authentication based on roles. Role-based authentication limits access to switch operations by assigning users to roles. There are two roles: network-operator and network-administrator. The network operator has permission to view the configuration only. The network administrator has permission to execute all commands and make configuration changes.

See Chapter 9, "Configuring Switch Security."

Tools for Software Configuration

You can use one of two configuration management tools to configure your SANs: the CLI and the Cisco MDS 9000 Family Fabric Manager graphical user interface. (See Figure 1-1.)

Figure 1-1 Tools for Configuring Software



CLI

With the CLI, you can type commands at the switch prompt, and the commands are executed when you press the Enter key. The CLI parser provides command help, command completion, and keyboard sequences that allow you to access previously executed commands from the buffer history.

Continue reading this guide for more information on configuring the Cisco MDS 9020 Fabric Switch using the CLI.

Cisco MDS 9000 Family Fabric Manager

The Cisco MDS 9000 Family Fabric Manager application is a set of network management tools that support secure Simple Network Management Protocol and legacy versions. It provides a graphical user interface (GUI) that displays real-time views of your network fabric and lets you manage the configuration of the Cisco MDS 9020 Fabric Switch. The Fabric Manager applications are as follows:

- Fabric Manager Server—Performs advanced monitoring, troubleshooting, and configuration for multiple fabrics. The server must be started before running the Fabric Manager. The server can be accessed by up to 16 Fabric Manager clients at a time.
- Device Manager—Presents the Device View of the a switch. Device View displays a continuously updated physical representation of the switch configuration and provides access to statistics and configuration information for a single switch.
- Fabric Manager Web Client—Allows operators to monitor MDS events, performance, and inventory from a remote location using a web browser.

The Cisco Fabric Manager applications are an alternative to the CLI for most switch configuration commands.

Refer to the *Cisco MDS 9000 Family Fabric Manager Configuration Guide*.